SACM Vulnerability Assessment Scenario

IETF 95

04/05/2016

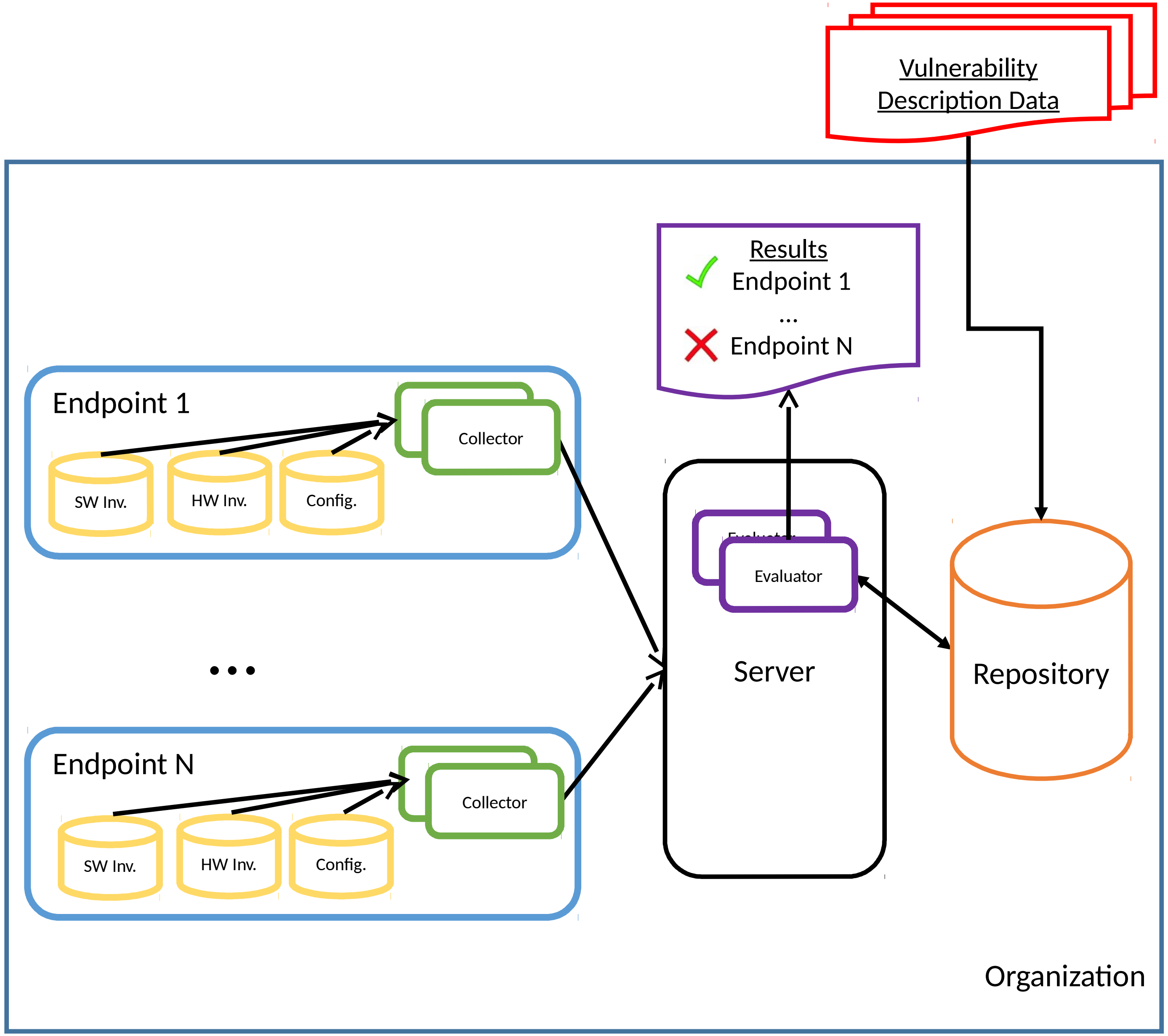
What is it?

- Operational use case for enterprise vulnerability assessment
  - Endpoint identification and initial data collection
  - Vulnerability description data
  - Endpoint applicability and assessment
  - Assessment results

- Begins with an enterprise ingesting vulnerability description data and ends with identifying affected endpoints

- Aligns with the SACM Use Cases[1] and builds upon the usage scenarios

[1] https://datatracker.ietf.org/doc/rfc7632/



Purpose

- Provides a detailed scenario and vision for enterprise vulnerability assessment that can be used as a core narrative
- Identifies aspects for use in the development of the information model
- Defines the classes of data, major roles, and a high-level description of role interactions
- Helps to further inform engineering work on protocol and data model development
- Part of the overall goal of breaking the SACM problem space into smaller and more manageable pieces

Scope and Assumptions

- Does not attempt to cover the security disclosure itself and any prior activities of the security researcher or discloser

- Assumes the vulnerability description data contains all information necessary to identify affected endpoints within an organization

- Assumes the vulnerability description data has been processed into a format that the enterprise security software tools can understand and use

- Assumes the enterprise has a means of identifying and collecting information from their enterprise endpoints

Endpoint Identification and Initial Data Collection

- Identifies and collects basic information from enterprise endpoints
  - Network identity
  - Operating system and patch level
  - Installed software inventory
  - …
- Occurs before receiving and processing any vulnerability description data
- Information should be stored within a repository
- Information obtained could be used by other enterprise processes, such as configuration and license management

Vulnerability Description Data and Endpoint Applicability and Assessment

- Vulnerability description data is received and tagged (e.g., internal ID) by the enterprise and stored for immediate or later use within a repository

- Data versions are tracked in the event that the data is updated at a later time

- In many cases, applicable or affected endpoints can be determined using the previously collected basic information and software inventory. No further assessment of data collection needed.

- If required, a secondary assessment is used to collect additional information such as:
  - Files and their attributes
  - Text configuration file settings
  - Windows registry queries
  - …

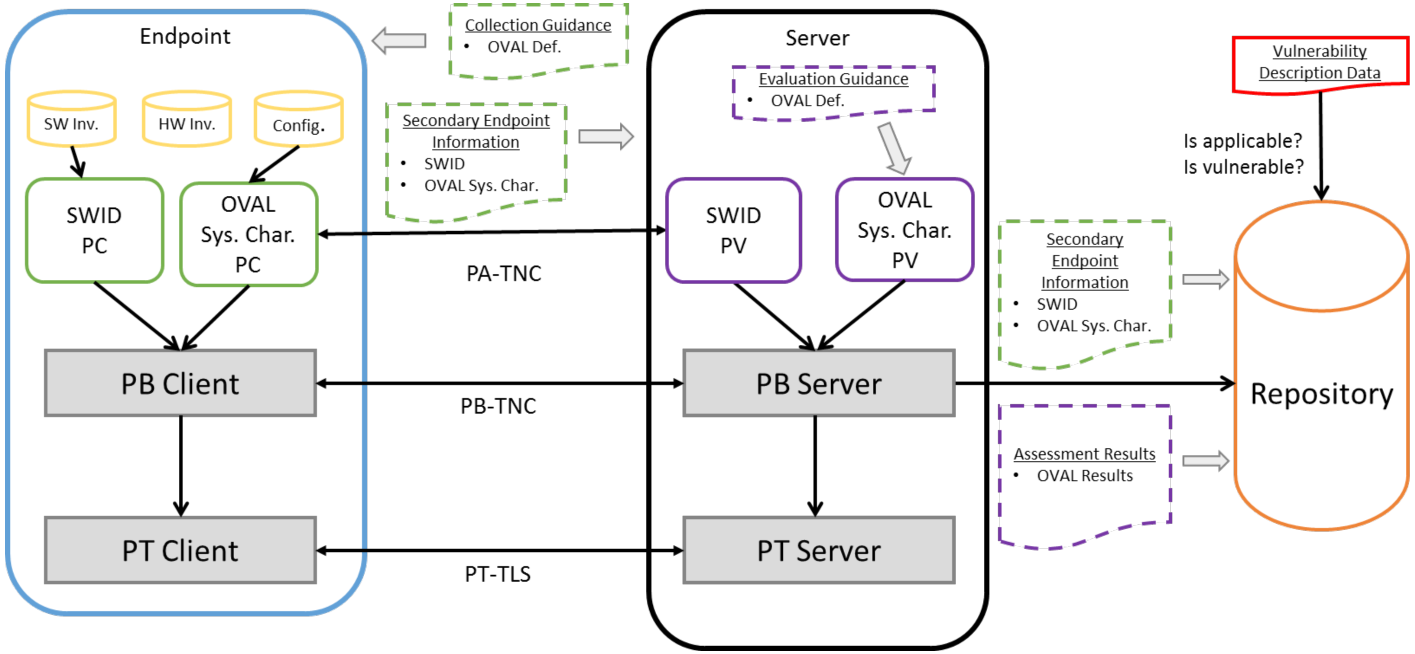
Assessment Results

- The results that determine which enterprise endpoints are applicable to the vulnerability description data

- Essential data items include (not the complete list):
  - Endpoint ID
  - Vulnerability description data
  - Date of assessment
  - Age of collection data
  - …

Solution I-Ds in progress

- Extensible transport framework (ECP[1], NEA[2])
- Software inventory (SWID M&A[3])
- Evaluation guidance, collection guidance, configuration information, and results (OVAL[4])
- Are there other standards we should look at?



1. https://datatracker.ietf.org/doc/draft-haynes-sacm-ecp/
2. https://datatracker.ietf.org/wg/nea/documents/ (see PA-TNC, PB-TNC, PT-TLS)
3. https://datatracker.ietf.org/doc/draft-coffin-sacm-nea-swid-patnc/
4. https://datatracker.ietf.org/wg/sacm/documents/ (see draft-*-sacm-oval-*-model). Also, please note where OVAL is mentioned, above, I really mean the next-generation data models based on OVAL :).

Wrap-up

- We would love to hear any feedback you have on the current draft

- TCG is interested in how TNC specifications can be applied to network devices
  - Other specifications of interest (Server Discovery and Validation[5] and IF-M Segmentation[6])
  - Historically has been very willing to transfer specifications to the IETF

1. https://www.trustedcomputinggroup.org/files/resource_files/3D59FB5E-1A4B-B294-D0F322A08B48E02E/Server_Discovery_And_Validation_v1_0r19-PUBLIC%20REVIEW.pdf
2. https://www.trustedcomputinggroup.org/files/resource_files/B17D87EF-1A4B-B294-D0B0A71BDAE2F3C3/IFM_Segmentation_v1r5_Public%20review.pdf

Appendix

- Additional processes that have not been integrated into the overall document
  - Continuous Vulnerability Assessment – timing of assessments (e.g., initial assessments, reassessments, etc.)
  - Priority – vulnerability description data and the remedies

- Data attribute table and definitions
  - A table of all discussed data attributes and where they are used, followed by their definitions

- Alignment with other works
  - The Council on CyberSecurity's Critical Security Controls
    - CSC 1 Inventory of Authorized and Unauthorized Devices
    - CSC 2 Inventory of Authorized and Unauthorized Software
    - CSC 4 Continuous Vulnerability Assessment and Remediation

Appendix (continued)

- Alignment with SACM Usage Scenarios
  - Automated Checklist Verification (2.2.2)
  - Detection of Posture Deviations (2.2.3)
  - Asynchronous Compliance/Vulnerability Assessment at Ice Station Zebra (2.2.5)